Audit Aplikasi Core Business Perusahaan Jasa Keuangan

Dewi Puspasari [1], M. Sattar [2], M. Kasfu Hammi [3]

[1,2,3]*Universitas Indonesia*
E-mail: dewi.puspa00@gmail.com, sattar@gmail.com, kasfu@gmail.com

ABSTRAK

Suatu sistem aplikasi disusun dalam rangka untuk memenuhi kebutuhan penggunanya. Untuk mengetahui kualitas kinerja sistem aplikasi terutama kaitannya dalam hal keamanan/kerahasiaan, ketersediaan, dan integritas data maka perlu dilakukan evaluasi secara berkala, berupa audit sistem informasi. Kebutuhan akan evaluasi kinerja aplikasi ini juga dirasakan oleh PT XYZ, suatu perusahaan negara yang bergerak di bidang jasa keuangan. Apalagi setelah aplikasi utama mereka dinilai kurang andal oleh Badan Pemeriksa Keuangan untuk melayani pelanggan mereka yang berjumlah jutaan peserta. Karena itu dalam penelitian ini kami melakukan audit sistem informasi dengan ruang lingkup aplikasi core business untuk mengetahui apakah aplikasi utama tersebut memiliki kontrol internal yang cukup untuk menjamin keandalan dan akuntabilitas layanan. Dari hasil penelitian kami dapat diketahui bahwa aplikasi core business tersebut masih memiliki beberapa kelemahan pada kontrol, terutama disebabkan kurangnya landasan operasional dan konsistensi dalam implementasi kebijakan dan prosedur terkait.

Keywords: audit, aplikasi *core business*, evaluasi, kontrol

1. PENDAHULUAN

Suatu aplikasi *core business* bagi perusahaan merupakan roda penggerak operasional. Apabila kualitas aplikasi tersebut rendah maka dapat menurunkan kinerja perusahaan tersebut, menurunkan kualitas layanan pelanggan, atau bahkan dapat menurunkan citra perusahaan tersebut di mata publik. Begitu pula apabila aplikasi *core business* telah dirasa matang (*mature*), suatu perusahaan tidak boleh langsung berpuas diri, melainkan harus selalu waspada dengan melakukan evaluasi kinerja aplikasi tersebut secara berkala karena ancaman pun terus meningkat.

Evaluasi terhadap kinerja aplikasi bukan merupakan sesuatu hal yang baru di Indonesia. Apalagi mengingat peranan teknologi informasi yang saat ini bukan hanya sebagai *support* melainkan berperan sebagai *enabler* perbaikan proses bisnis perusahaan dan sarana membantu pengambilan keputusan (Hinarto dkk, 2009; Tarigan dkk, 2010).

Penilaian ini dilakukan suatu organisasi secara berkala untuk mengetahui kualitas kinerjanya dari berbagai aspek, mulai dari kecepatan akses, kenyamanan bagi pengguna, keakuratan output aplikasi, dan sebagainya. Apabila evaluasi tersebut bertujuan untuk mengukur keandalan kontrol internal dan efektivitas sistem untuk mencegah terjadinya manipulasi maka evaluasi ini disebut audit sistem informasi. Di Indonesia, audit ini umumnya dilakukan oleh satuan pengawas internal dan audit eksternal. Ruang lingkup audit sistem informasi ini dapat ditentukan sesuai kebutuhan dan kepentingan organisasi, apakah meliputi keseluruhan perangkat TI di organisasi tersebut (*general audit*) atau berfokus pada suatu aplikasi tertentu (*application audit*)

Oleh karena itu pada penelitian kali ini kami akan melakukan audit aplikasi *core business* suatu perusahaan yang bergerak di bidang jasa keuangan. Perusahaan ini menganggap penting adanya kegiatan audit aplikasi oleh pihak eksternal karena adanya keraguan Badan Pemeriksa Keuangan (BPK) terhadap keandalan dan akuntabilitas aplikasi ini dalam melayani pelanggan mereka yang telah mencapai jutaan peserta. Dengan adanya audit dari pihak ketiga diharapkan permasalahan dan hasil temuan dapat lebih detail dan obyektif karena BPK tidak menjelaskan secara detail dan spesifik sumber keraguan mereka. Dari temuan hasil audit tersebut maka ke depannya dapat dilakukan perbaikan untuk peningkatan efektivitas aplikasi *core business* tersebut.

2. TINJAUAN PUSTAKA

2.1. Audit Sistem Informasi

Data bagi suatu perusahaan merupakan sebuah aset yang berharga. (Dewald, 2013) Keandalan data dan sistem informasi menjadi perhatian utama para auditor, termasuk di antaranya kontrol internal yang melekat sistem tersebut. Selain untuk efisiensi, tujuan adanya kontrol internal tersebut untuk meminimalkan risiko kerugian karena kesalahan, manipulasi, tindakan ilegal dan insiden yang menyebabkan sistem menjadi tidak tersedia (GAO, 2009).

Untuk mengukur keandalan kontrol internal dan proses-proses untuk memastikan kecukupan kontrol tersebut maka dilakukan kegiatan audit sistem informasi. Menurut Ron Webber (2010) audit sistem informasi (SI) perlu dilakukan secara berkala, di antaranya disebabkan hal-hal sebagai berikut: kerugian akibat kehilangan data, kesalahan dalam pengambilan keputusan, risiko kebocoran data, penyalahgunaan sistem, kerugian akibat kesalahan proses perhitungan, serta tingginya nilai investasi perangkat keras dan perangkat lunak teknologi informasi (TI).

Gondodiyoto & Hendarti (2006) mendefinisikan audit SI sebagai proses pengumpulan dan penilaian bukti untuk menentukan apakah sistem komputer perusahaan mampu mengamankan harta, memelihara kebenaran data, dan mampu meraih tujuan

perusahaan secara efektif. Audit SI mampu memberikan evaluasi yang bersifat independen atas kebijakan, prosedur, standar, pengukuran, dan praktik untuk menjaga/mencegah informasi yang bersifat elektronik dari kehilangan, kerusakan, penelusuran yang tak disengaja, serta memberikan pendekatan holistik untuk mengindentifikasi dan mengaluasi sumber daya dan alur informasi organisasi dengan tujuan untuk mengorganisasi sistem informasi organisasi secara efektif dan efisien (GAO, 2009 dan Steven & Gib, 2007). Ada tiga kontrol utama yang dievaluasi pada aktivitas audit yaitu ketersediaan data *(availability*), kerahasiaan (*confidentiality*), dan integritas *(integrity)* data (GAO, 2009 dan Gondodiyoto & Hendarti, 2006).

Secara umum audit sistem informasi terbagi menjadi dua, yakni audit secara umum (*general audit*) dan audit terhadap keamanan perangkat lunak, yang lebih umum dengan sebutan audit kontrol aplikasi atau audit aplikasi (GAO, 2009). Audit umum (*general audit*) dapat dilakukan baik oleh auditor internal maupun auditor eksternal di tiap-tiap perusahaan secara berkala. Sementara audit aplikasi umumnya dilakukan berdasarkan kebutuhan perusahaan. Kedua jenis audit tersebut saling terkait. Kualitas kontrol sebuah aplikasi yang buruk akan mempengaruhi penerapan kontrol dalam meminimalkan risiko teknologi informasi secara umum. Sebaliknya, kurangnya komitmen perusahaan terhadap penerapan regulasi dan kontrol internal juga mempengaruhi penerapan kontrol dalam lingkup aplikasi (GAO,2009).

2.2. Audit Aplikasi

Kontrol aplikasi didefinisikan oleh General Accounting Office (2009) sebagai kontrol untuk mencapai sasaran atas akurasi, kelengkapan, keabsahan/validitas, kerahasiaan, serta ketersediaan transaksi dan data selama pengolahan aplikasi.

Kontrol aplikasi ini terbagi menjadi empat kategori kontrol, yaitu kontrol umum tingkat aplikasi, kontrol proses bisnis, kontrol antarmuka, dan kontrol sistem manajemen data. Kontrol umum tingkat aplikasi merupakan kontrol umum (*general control*) yang beroperasi pada tingkat aplikasi, termasuk di antaranya manajemen keamanan, kontrol akses, manajemen konfigurasi, pemisahan tugas, dan perencanaan kontingensi (*business continuity plan*)

2.3. Panduan Audit Aplikasi

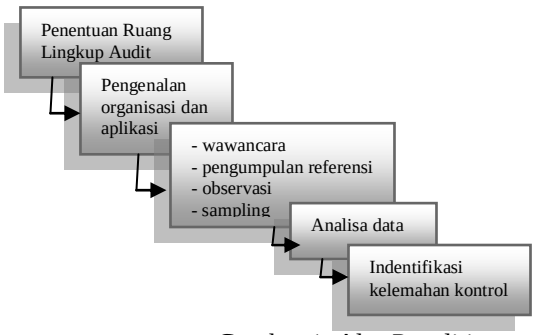
Ada beberapa panduan audit yang umum digunakan, seperti Control Objectives for Information and Related Techology (COBIT), ISO 27001/27002, Information Technology Infrastructure Library *(*ITIL), dan Federal Information System Control Audit Manual *(*FISCAM). Dalam penelitian ini kami menggunakan pendekatan FISCAM yang dipublikasikan oleh General Accounting Office, badan pemerintah Amerika Serikat yang berfungsi seperti Badan Pemeriksa Keuangan.

FISCAM menyajikan suatu metodologi untuk melakukan audit kontrol sistem informasi berdasarkan standar profesional. Ada enam kategori kontrol umum yang dapat diaplikasikan di level entitas/organisasi atau level aplikasi, yaitu sebagai berikut:

1. Pengelolaan keamanan, yaitu mulai dari membangun kebijakan keamanan, membagi tanggung jawab, dan mengawasi kelemahan kontrol keamanan.
2. Kontrol akses, berkaitan dengan pembatasan penggunaan sumber daya komputer termasuk perlindungan dari adanya penyusup.
3. Kontrol perubahan dan pengembangan aplikasi, yakni melindungi aplikasi yang eksis dari adanya modifikasi yang tidak terotorisasi.
4. Kontrol *software* sistem, berkaitan dengan pembatasan dan pengawasan terhadap program dan file melalui monitoring terhadap hardware dan aplikasi yang didukung oleh sistem. Kontrol ini bisa dibedakan atas kontrol aplikasi dan kontrol proses antar aplikasi.
5. Pemisahan tugas, berkaitan dengan kebijakan, prosedur, dan struktur organisasi sehingga setiap tidak terjadi rangkap jabatan yang membuat seseorang mampu memodifikasi aplikasi atau data dengan tidak terotorisasi.
6. Kontrol kontinuitas layanan, untuk memastikan operasi bisnis yang kritis tetap berjalan meski terjadi interupsi, termasuk tetap terlindunginya data yang sensitif.

3. METODOLOGI

Audit sistem informasi pada PT XYZ difokuskan pada aplikasi *core business*. Untuk melakukan audit aplikasi tersebut kami melakukan tahapan seperti pada Gambar 1.



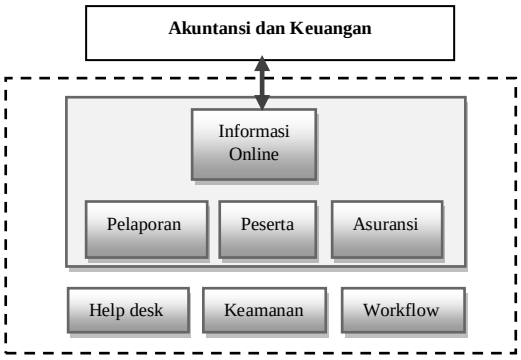
Gambar 1. Alur Penelitian

Setelah mengetahui ruang lingkup audit kami mempelajari aplikasi tersebut serta mempelajari profil organisasi terutama sasaran, sifat bisnis/operasional dan kultur organisasi tersebut. Setelah itu kami melakukan wawancara terhadap tiap-tiap kepala bagian TI dan staf senior berdasarkan panduan FISCAM yang kami kustomisasi. Hasil wawancara ini kami cocokkan dengan kondisi praktik di lapangan serta dokumen/referensi seperti kebijakan TI, *Standard Operating Procedure* (SOP), panduan manual aplikasi dan panduan teknis operasional lainnya. Untuk menguji keandalan kontrol kami juga lakukan sampling ke beberapa modul aplikasi. Dari aktivitas-aktivitas tersebut (wawancara, studi dokumen, observasi, dan sampling) kami lakukan kesimpulan berupa kontrol-kontrol yang masih lemah.

4. HASIL DAN PEMBAHASAN

4.1. Profil Aplikasi Core Business

Aplikasi *core business* milis perusahaan jasa keuangan PT XYZ merupakan sistem aplikasi yang mendukung bisnis utama. Proses-proses yang direpresentasikan ke dalam modul-modul aplikasi *core business* tersebut di antaranya modul peserta, modul asuransi, dan modul pelaporan, serta modul informasi online. Modul asuransi merupakan modul utama karena di dalamnya memuat beragam asuransi yang ditawarkan oleh perusahaan XYZ ke masyarakat, di antaranya asuransi kematian, kecelakaan kerja, dan asuransi hari tua. Modul-modul tersebut berhubungan dengan modul akuntansi dan keuangan, yang terdiri dari submodul anggaran dan hutang-piutang. Selain modul-modul tersebut, aplikasi *core business* ini juga memiliki modul-modul pendukung, seperti modul bantuan (help desk), keamanan, dan modul alur kerja (*workflow*). Modul-modul dalam aplikasi *core business* dapat dilihat pada Gambar 2. Aplikasi *core business* ini dikembangkan dengan menggunakan *platform* teknologi Oracle, menggunakan database terpusat, dan arsitektur *three tier* yang memisahkan antara proses *client*, aplikasi, dan *database*.



Gambar 2. Modul-modul Aplikasi *Core Business*

4.2. Hasil Rekapitulasi Wawancara, Observasi, dan Referensi Dokumen

Audit aplikasi ini kami lakukan dengan menggunakan pendekatan FISCAM. Daftar pertanyaan tersebut kami ringkas sehingga total menjadi 75 dari 163 teknik kontrol. Peringkasan ini disebabkan adanya redundasi/pengulangan pernyataan dan disesuaikan dengan ruang lingkup aplikasi. Hasil rekapitulasi wawancara, pengumpulan referensi, dan observasi di antaranya dapat dilihat pada Tabel1.

Tabel 1. Hasil Rekapitulasi

Mekanisme Kontrol	Penjelasan	Referensi
Pengaturan Akses Aplikasi		
Adanya ketentuan hak akses bagi setiap pengguna yang disesuaikan dengan kewenangan	PT XYZ telah memiliki ketentuan hak akses berdasar wewenang, namun terkadang di-*by pass* sehingga data hasil verifikasi data kurang akurat.	Kebijakan Keamanan Informasi: Standar Pengendalian Akses Aplikasi dan Standar Account Management
Manajemen Konfigurasi Aplikasi		
Adanya kebijakan dan prosedur untuk memastikan bahwa setiap modifikasi pada aplikasi telah	Kebijakannya telah ada, namun praktiknya belum ada penanggung jawab	Kebijakan dan prosedur pengelolaan perubahan, mencakup kategorisasi, prioritasi, prosedur darurat, dan

mendapat persetujuan	konfigurasi dan perubahan aplikasi, serta tidak adanya dokumentasi terhadap perubahan konfigurasi aplikasi yang telah dilakukan.	pengelolaan rilis.
Pemisahan Kewenangan Pengguna		
Penanggungjawab layanan telah mengidentifikasi peran-peran pengguna sistem yang tidak boleh dirangkap	PT XYZ belum melakukan identifikasi peran-peran pengguna sistem yang tidak boleh dirangkap.	-
Kontrol Aplikasi		
Aplikasi harus dapat dikonfigurasikan untuk menolak data input yang tidak memenuhi ketentuan.	Beberapa kontrol aplikasi masih lemah untuk form-form utama, seperti *field* No peserta yang bisa diisi semua karakter.	Hasil *sampling* dan buku manual aplikasi
Proses Antar Aplikasi		
Adanya mekanisme untuk mencegah terjadinya pertukaran data yang sama lebih dari sekali (duplikasi)	Secara umum kontrol terhadap duplikasi tersebut telah cukup	Hasil *sampling*
Manajemen Keamanan Data		
Adanya fasilitas monitoring dan *logging* untuk memantau dan mencatat aktivitas yang melibatkan akses ke data	Sudah ada fasilitas logging, namun log tersebut jarang di-*review*	Kebijakan pengelolaan sumber daya TI
Kontinuitas Layanan		
Adanya *backup* dari file aplikasi yang digunakan saat ini	Saat ini telah ada *backup* server aplikasi namun belum ada *backup* core switch, sehingga berpotensi terjadi *single point of failure* jika core switch rusak.	Kebijakan pengelolaan sumber daya TI

4.3. Hasil Sampling

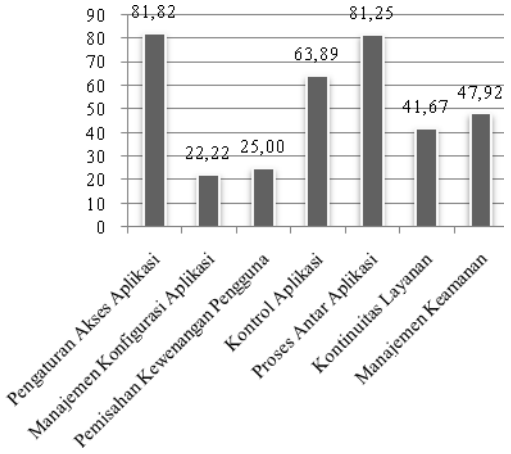
Kami melakukan *sampling* ke beberapa *form* utama, di antaranya *form* registrasi pelanggan, *form* calon pelanggan potensial, dan *form* klaim. Pemilihan form untuk sampling ini berdasarkan hasil wawancara terhadap kepala help desk dan kepala bagian aplikasi *core business* yang menyebutkan bahwa *form* ini kerap mengalami permasalahan, seperti adanya input nama peserta yang terduplikasi dan output yang dinilai kurang akurat. *Sampling* kontrol input pada *form* tersebut bertujuan untuk memastikan apakah kontrol input yang diperlukan sudah cukup. Kontrol input yang dilakukan di antaranya berupa: *limit check*, *duplicate check*, *validity check*, *hash total*, *table lookups*, *existence check*, dan *completness check*. Berdasarkan hasil uji *sampling* tersebut, kontrol input pada form tersebut cukup baik, namun ada beberapa yang digarisbawahi, yaitu:

1. Format dan standar baku nomor induk pegawai. Nomor induk pegawai peserta seharusnya merupakan *key field* sehingga seharusnya ada format khusus untuk pengisian dan aturan tidak boleh adanya duplikasi, karena nomor induk pegawai bagi peserta merupakan *field* yang unik. Saat dilakukan pengujian, nomor ini bisa diisi karakter angka, huruf, maupun karakter khusus (*wildcard*), boleh tidak diisi, dan dilakukan duplikasi.
2. Nomor identitas seperti KTP dan STNK merupakan sesuatu yang unik. Oleh karena itu aturan tidak boleh adanya duplikasi seharusnya diterapkan dalam kontrol input *form* ini.
3. Proses *upload* tidak memiliki kontrol untuk mengidentifikasi format file teks yang akan di-*upload.* Artinya semua jenis file teks masih dapat dimasukan. Sehingga berpotensi untuk masuknya data-data yang tidak valid ke dalam basis data.
4. Fungsi tombol 'Cetak Tanda Terima' tidak dapat berfungsi dengan baik, karena aplikasi menjadi *hang*, sehingga tidak dapat diproses.

4.4. Temuan Audit Aplikasi

Berdasarkan rekapitulasi aktivitas-aktivitas audit aplikasi tersebut maka dapat disimpulkan bahwa PT XYZ telah memiliki kebijakan terkait dengan pengelolaan aplikasi *core business*, namun sebagian di antaranya belum memiliki prosedur pelaksanaan, fungsi TI terkait aktivitas tersebut, dan belum dilaksanakannya aktivitas tersebut secara konsisten. Dari keenam kategori kontrol tersebut, pemenuhan kontrol dapat dilihat pada gambar 3. Kami memberikan poin 0-1, dimana poin 0 berarti

belum sama sekali dilakukan; 0.25-0.5 jika telah memiliki kebijakan namun belum dilakukan atau belum memiliki prosedur; 0.75 jika telah memiliki kebijakan namun belum diimplementasikan secara konsisten; dan 1 jika kebijakan dan prosedur lengkap, serta telah diimplementasikan secara konsisten.



Gambar 3. Persentase Pemenuhan Kontrol Tiap Kategori Kontrol

Dari gambar 3 terlihat bahwa manajemen akses aplikasi pada PT XYZ telah cukup baik (81,82%) disusul kontrol pada proses antar aplikasi (81,25%) dan kontrol aplikasi (63,89%). Kategori kontrol yang buruk (22,22%) yaitu pada manajemen konfigurasi aplikasi karena belum dilaksanakannya *update* dokumen apabila terjadi perubahan, serta belum adanya penanggung jawab terhadap aktivitas ini. Sedangkan pemisahan wewenang pengguna belum menjadi isu pada organisasi XYZ sehingga belum ada kajian terhadap permasalahan tersebut. Kontrol pada kontinuitas layanan mendapat skor 41,67% karena aktivitas ini tidak di-*review* secara berkala dan koordinasinya masih bersifat sporadis. Sedangkan kontrol pada keamanan data belum maksimal (47,925) karena *database* operasional dan ujicoba masih menjadi satu serta masih bisa dilakukan akses data langsung pada *database*, selain itu juga tidak dilakukan *review* dan validasi secara berkala terhadap master data.

5. SIMPULAN

Kontrol internal untuk aplikasi *core business* PT XYZ masih memiliki kelemahan-kelemahan dimana apabila tidak segera ditindaklanjuti akan mengganggu kinerja operasional dan akuntabilitas layanan bisnis utama. Kelemahan kontrol tersebut di antaranya disebabkan kurangnya prosedur atau landasan operasional, belum didefinisikannya penanggung jawab aktivitas tertentu, dan belum diimplementasikannya kebijakan secara konsisten. Di antara kategori kontrol umum level aplikasi tersebut, kontrol pada manajemen konfigurasi aplikasi paling lemah sehingga proses perubahan dan perbaikan aplikasi yang telah dilakukan sulit ditelusuri.

DAFTAR PUSTAKA

Buchanan,S. dan Gib, F. The Information Audit: Role and Scope. 2007. *International Journal of Information Management 27: 159-172.*

Dewald, P. 2013. *Exploding the Myth of "Data is an Asset*. (Online). (http:// http://dataqualitypro.com/data-quality-pro-blog/data-is-an-asset-myth-diaku diakses pada 15 September 2013).

GAO. 2011. *FISCAM Objective*.

GAO. 2009. *Federal Information System Controls Audit Manual*.

Gondodiyoto, S., dan Henny, H. 2006. *Audit System* Informasi. Jakarta: Mitra Wacana Media

Hall, J.A. 2011. *Information Tec Auditing & Assurance*. Lehigh Univ, South Western Cencage.

Hinarto, S., Setiawan D., dan Septiano, Y. 2009. *Analisa Investasi Sistem dan Teknologi Informasi dengan Menggunakan Metode New Information Economics pada Bank XYZ.* Skripsi Tidak Diterbitkan. Jakarta: Ubinus.

Tarigan, J., Purbo O., dan Sanjaya, R. 2010. *Business-Driven Information System: dari Techology Age Menjadi Information Age Menuju Co-Creation Age*. Jakarta: Elex Media Komputindo.

Weber, R. 2000. *Information System Control and Audit*. New Jersey: Prentice Hall.